The HIPAA Implementation Newsletter
Issue #47 – Friday, November 29, 2002
| Compliance | Business Associates | Security | Privacy | Hospitals |
Web format with links at http://lpf.com/hipaa

Commentary: HIPAA Compliance Doesn't Come In a Box

"… HIPAA, in large part, was a sleeping giant until this year. The organizations that must comply with HIPAA are now realizing that something must be done about this beast. The problem is that the majority of these covered entities -– the smaller health care practices and their business associates -– don't have a clue about how to get started with their compliance efforts.
"Vendors have seen a great opportunity to capitalize on this general lack of awareness and know-how, and have begun offering canned HIPAA solutions. These solutions range from practice management systems to firewalls and data encryption products to electronic transaction clearinghouse services. Regardless of the solution, there seems to be a common sales pitch, and even worse, a common misconception on the customer's part that these solutions will, in one motion, make an organization 'compliant.' This belief is a misnomer at best, and those who buy into it could be making a critical mistake.
"HIPAA compliance cannot be bought.
"Sure, covered entities will have to buy products and services, and they will have to search out expertise to assist with their compliance efforts. It's just that HIPAA readiness and ongoing compliance is not about technical solutions or IT in general. Some of the products on the market are valuable and can be integrated into an overall compliance plan. However, health care organizations cannot simply throw money at their HIPAA initiatives, buy a few products, and think that the result will be HIPAA compliance.
"Technology only provides a way to enforce policies and assist with procedures. A firm's HIPAA efforts should be focused on integrating policies and procedures with business processes.
"HIPAA involves most, if not all, health care business processes. More specifically, HIPAA is a business problem that involves people. As with anything, when people are introduced into the equation, things become vastly more complicated. HIPAA requires policies, procedures, training and more. It also requires strategic planning, project management, maintenance, auditing, risk management, customer relations, legal issues and financial considerations -- practically everything that comes with running a business.
"HIPAA compliance is not a one-time deal. It will require ongoing efforts that have to be managed wisely. If you or someone you know is affected by HIPAA, do yourself and your customers a favor and make sure that you find out for yourself what you have to do to prepare for and maintain HIPAA compliance. Concern for the privacy and security of patient information is, after all, a major factor in the HIPAA legislation. These concerns should be seen as part of a basic business strategy and not just something health care organizations are forced to do because of government regulations.
"To get the HIPAA ball rolling … do some research and learn what exactly it is going to take to reach and maintain compliance, so you'll be educated and prepared when the vendors come knocking. In other words, trust what you know yourself, not what someone else tells you. Remember, no matter what anyone says, HIPAA compliance does not come in a box."
+ More at:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci857626,00.html
By Kevin Beaver, special to SearchSecurity.com

Business Associates: Compliance Date II

We have said many times that we are not attorneys and do not give legal advice. That doesn't keep us from being troubled by some of the advice we read about interpretations of the HIPAA regulations. With our clients, we recommend assuming that the most conservative point of view is correct until you have received an opinion from legal counsel.

In issue #40, August 23, 2002 we carried a number of articles about the second round of HIPAA privacy regulations. One article, *Business Associates: Compliance Date* cited an article from PricewaterhouseCoopers that says in part, 'This delay is not available in situations where no written contract exists as of October 15, 2002. An employer that does not have an existing written arrangement with a vendor must have a written business associate contract in place by April 14, 2003 with that vendor. Similarly, any qualifying contract that comes up for renewal or renegotiation prior to April 14, 2004 must meet the business associate requirements when the renewal or renegotiations are finalized, even if that date is prior to April 14, 2004.' There are two articles included in this issue that suggest that the April 14, 2004 date is universally applicable. We encourage you to check with legal counsel about the effective dates for business associates compliance.

http://lpf.com/hipaa/issue40.html#bus-assoc-compliance-date-#40

Business Associates: Chain of Trust

"… the final security rule due out December 27 will require facilities to include chain of trust clauses in their business associate agreements, instead of developing separate contracts. The clause will not be necessary at all in business associate agreements with organizations that are also covered entities, because the law already requires them to have their own security in place, says Braithwaite, national director of HIPAA advisory services at PricewaterhouseCoopers, and former senior advisor on health information policy for HHS.
We hate to counsel delays in HIPAA preparedness, but this suggests that delaying the signing of business associates agreements may be prudent. Check with legal counsel.
+ More at: http://www.hipaadvisory.com/news/ November 25, 2002

Security: Federal Government

"Overall, federal agencies earned an 'F' on Rep. Stephen Horn's latest report card on government security — the same grade they earned in 2001. Of the 24 federal agencies Horn graded, 14 flunked. The highest grade was a B-minus.
"During the final hearing of his subcommittee Nov. 19, Horn offered a shred of faint praise for the computer security efforts of the agencies he graded. 'Eleven of the 24 agencies have shown some improvement,' he said. But 'overall, progress is slow.' Some agencies seem to be 'getting a handle on the scope of their computer security problems, but in the meantime, the federal government's systems and assets remain vulnerable.'"
"But even as agencies begin to understand the scope of their problems, the problems are getting worse, he said. 'Reports of attacks and disruptions are growing, and they are becoming more complex and harder to trace. The number of reported computer security incidents has risen 71 percent over the last year.'" Horn gave the Department of Health

and Human Services a “D-.”
+ More at: http://www.fcw.com/fcw/articles/2002/1118/web-horn-11-20-02.asp

Privacy: Database

“Privacy and American Business (P&AB) has developed a new searchable Privacy Policy Database, which will allow those managing privacy to benchmark their own privacy policy status. The Database will be unveiled at P&AB’s upcoming Privacy Leadership Group Briefing and Workshop December 5-6 in Washington, D.C.
“… the database is a compilation of consumer privacy policies from companies across different industries including banking, credit and consumer cards, consumer reporting, **health, insurance**, investments, **pharmaceuticals**, and telecommunications. It is searchable by industry, location, opt-in/opt-out, offline/online, consumer response method, availability of a contact person, such as a CPO, for consumer redress, and more. For each industry, exemplary policies will be flagged, with a discussion why it is outstanding, and how it may be adapted.
“The database will not only house privacy policies, but will also include vital information on the legislation that drives privacy policies like GLB, **HIPAA**, and COPPA. Guides to writing privacy policies and using the database will also be provided to users. This web-based database will be updated quarterly and housed at www.pandab.org.
+ More at: http://www.pandab.org/privacydbrelease.html

Privacy: Iowa Dead Baby II

Completing another article in Issue #40: “The Iowa Supreme Court has dismissed a high-profile case involving pregnancy records in Storm Lake, leaving a landmark legal fight in the same place as the baby death investigation that started it: unresolved. …
“The county dropped out of the case earlier this month. The Supreme Court declared the case moot Wednesday, despite Planned Parenthood's request that justices move forward in case a similar situation arises in the future. …
“The legal battle drew national attention, split Storm Lake residents and baffled legal experts. The debate centered on the definition of medical records… Planned Parenthood officials said pregnancy records are protected by state and federal privacy laws. [The county] argued that the records aren't private because clinic employees who distribute pregnancy tests don't have to be doctors or nurses. …
“‘It doesn't mean those issues aren't still out there,’ said Bob Rigg, a Drake University law professor. ‘It simply means they haven't been resolved.’”
+ More at: http://www.pandab.org/privacydbrelease.html

Privacy: Cost Savings and the Cost to Privacy

“‘A new tactic in what has been a losing battle against rising health insurance premiums for Colorado companies is emerging in the state this fall, and employees' privacy may be the cost. …
“The concept, known as outcomes management - not to be confused with disease management, which health insurers for years have used to categorize members as ‘asthmatics’ or ‘diabetics’ - is saving millions of dollars from corporate budgets and drastically improving the lives of the nation's sickest individuals, proponents say. But no matter how beneficial, the technology's price is privacy, say critics, who warn that as

employers gain access to the intimate details of workers' lives, they also gain a tool for discrimination. …
“Even with a host of new federal privacy laws prohibiting personally identifiable information from being released to the wrong hands, lawmakers and health management program developers are interpreting the law as one that allows employers to see reports detailing the age and gender of their most expensive medical cases and assign those employees to medical caseworkers.
“Employers can get information from medical bills and health plan records, which can be very detailed, even showing what type of doctor a member requests during a call to a help line. ‘It sounds like Big Brother watching health care in the workplace,’ said Lorez Meinhold, executive director of the Colorado Consumer Health Initiative, who is particularly concerned about mental health information being used by employers to discriminate.
“Under a new federal privacy law scheduled to take effect in April as part of the Health Insurance Portability and Accountability Act, or HIPAA, employers can access employee medical information as long as details such as name, address, ZIP code, Social Security number and other identifiers are removed, said Gerald Niederman, an attorney for Faegre & Benson in Denver.
“However, there are limits to de-identification, Niederman said. If an employee is involved in a dispute with his employer over worker's compensation benefits, for example, the company has the right to see that employee's medical records. And in smaller companies, it's not too tough to figure out who the 54-year-old male who has had two heart attacks in the past two years is, experts say….
“Under the new HIPAA regulations, workers can request that doctors or health plans not release personal information to employers. But federal law only requires health providers to consider the request. They don’t have to honor it, he said.”
We say, check with your legal counsel. This article does a good job of laying out the issues. We see it as a strong argument for the privacy requirements of HIPAA.
+ More at:
http://www.denverpost.com/Stories/0,1413,36%257E33%257E979848,00.html?search=filter

What HIPAA Means to Hospitals

“Donald Ribelin, senior applications analyst with FirstHealth of the Carolinas, predicts that some of the toughest challenges hospitals have ahead of them when it comes to the Health Information Portability and Accountability Act will be cultural, not technical, in nature.

“Dave Kirby likewise believes that the cultural changes unleashed by the HIPAA privacy rules may prove problematic for some providers. Kirby, the information security officer with Duke University Medical Center in Durham, N.C., says that when it comes to medical information access, most clinicians have no complaints with the status quo, and are somewhat wary of change.

“This attitude may lead to some bumps in the road at the hospital level, Kirby says. ‘They don't necessarily see what's wrong with privacy right now,’ he says. ‘They're used to the information being controlled by the provider, so it may take a while for them to understand that the balance of power is shifting toward the patient.’

“The privacy regulations, however-the first of the HIPAA mandates to take effect with a deadline of next April-represent more than just a cultural challenge for hospitals. Experts

say that a range of procedural issues, including how protected health information can be shared between hospitals and their newly defined 'business associates'-i.e., credentialed physicians, laboratories and other third-party providers-leave plenty of room for interpretation, and confusion.

"'You can get yourself all tied up in knots trying to read the rule and figure out exactly what the circumstances are that constitute a business associate relationship,' says Roy Rada, a professor of healthcare information systems at the University of Maryland, Baltimore County. Fortunately, the publication of the final privacy rule in August gave providers an extra year, until April 2004, to codify their business-associate contracts.

"While experts say that most of the nation's larger hospitals and systems are making solid progress toward satisfying the full spectrum of HIPAA mandates, smaller facilities are having a harder time.

"'We're seeing a great disparity between these large organizations that have a wide range of intellectual and financial resources, and the 25-bed hospital in a rural area, where you might have one person who can barely change a computer tape, and where the financial resources are very tight,' says Holt Anderson, executive director of the North Carolina Healthcare Information and Communications Alliance, a nonprofit healthcare information technologies research and development consortium.

"Making matters worse, the cost of compliance per bed for smaller hospitals may be as much as double what it is for larger facilities, due to the economies of scale that larger organizations enjoy, says Rada. He estimates the cost of compliance for large-to-medium-size hospitals for the first year-costs that include everything from staff training to software modification and testing-at $800 per bed versus $1,600 for small facilities. The numbers were based on a HIPAA cost survey conducted by the HIPAA Advisory, a service provided by Phoenix Health Systems.

"'It's shocking that smaller entities are apparently having to bear a disproportionately large proportion of compliance costs,' Rada says. 'That certainly wasn't the intent of the legislation. The rule was very specific about providing flexibility to allow providers to determine what is reasonable.'

"Rada and others say that all providers, but most especially smaller facilities, should work together to achieve a consensus about what constitutes a reasonable approach to compliance. Aside from potentially lowering costs, determining and adhering to generally accepted compliance solutions may prove critical in thwarting litigation down the road.

"'In the end, it's going to be the courts and judges that will decide what is reasonable and appropriate,' says Anderson. 'So the danger is that if you're outside the norm, you'll be judged against your peers as to what you should have done.'

+ More at:
http://www.healthleaders.com/magazine/feature1.php?contentid=39757&CE_Session=59243c35cf0fecf17f6788c127a22de5

Note: This story is the third in a three-part series on the impact of HIPAA regulations on healthcare providers and insurers. Previous articles in the series have addressed how the regulations will affect physicians and health plans.

Update

We have added a link to Health Safety Information on our Privacy and Security page. http://lpf.com/hipaa/privacy-security.html#health-safety

Conferences

Office of Civil Rights to respond to questions re: HIPAA privacy rule implementation and enforcement during national hipaa summit audio conference -- Registrants able to submit advanced questions at: questions@hipaaaudioconferences.com -- Dec. 5, 2002, Thursday-- 10:00 am - 11:30 am PST -- 12 Categories Of Continuing Education Credit Offered http://www.hipaaaudioconferences.com
THE SIXTH NATIONAL HIPAA SUMMIT *The Leading Forum on Healthcare Privacy, Confidentiality, Data Security & HIPAA Compliance* March 26 - 28, 2003 Washington DC More information and links to presentations at past conferences: http://www.hipaasummit.com

---